REMARKS

Applicants have received an Office Action dated November 3, 2004 and a duplicate Office Action dated November 5, 2004, which are referred herein as the Office Action. The Applicants wish to thank the Examiner for updating the correspondence address and providing the duplicate Office Action.

Applicants have identified several issues in the Office Action to which attention is required. First, the Sprague et al. reference cited in paragraph 3 of the Office Action refers to the U.S. PG Publication number of the Okamoto et al. reference given in the final office action dated October 14, 2003. Clarification to the Notice of References Cited that indicated the correct reference for Sprague et al. was necessary. Second, in paragraph 18 of the Office Action, the Examiner refers to "Schenk et al's inventive concept" in his conclusion statement of the same paragraph alleging a motivation to combine the Venkatachary et al. and Sprague et al. references. Applicants again note that the same language appeared in the same location of the final office action dated October 14, 2003. Third, Applicants can discover no reason why previous amendments to the claims, some of which have been twice amended at this point, are not cited or referred to in arguments made by the Examiner. Applicants encounter difficulty responding to the Examiner's allegation that the prior art references teach or suggest all claim limitations when the Examiner refers to pre-amendment claim language.

Furthermore, Applicants remind the Examiner of his duty under section 706.02(j). "After indicating that the rejection is under 35 U.S.C. 103, the examiner should set forth in the Office action:
(A) **the relevant teachings** of the prior art relied upon, preferably with reference to the relevant column or page number(s) and line number(s) where appropriate,
(B) **the difference or differences** in the claim over the applied reference(s),
(C) the proposed modification of the applied reference(s) necessary to arrive at the claimed subject matter, and
(D) **an explanation** why one of ordinary skill in the art at the time the invention was made would have been motivated to make the proposed modification." (emphasis added)

Applicants submit that by performing essentially a "copy and paste" from the final office action dated October 14, 2003, the Examiner has not satisfied his initial burden "to provide some suggestion of the desirability of doing what the inventor has done." MPEP 706.02(j). "Where a reference is relied on to support a rejection, whether or

not in a minor capacity, that reference should be positively included in the statement of the rejection. See In re Hoch, 428 F.2d 1341, 1342 n.3 166 USPQ 406, 407 n. 3 (CCPA 1970)." Id. "It is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to reply." Id.

Rejection Under 35 USC 103(a)

In paragraph 3 of the Office Action, the Examiner rejected claims 1-15, 17-62, 64-80, and 82-88 under 35 U.S.C. §103(a) as being unpatentable over the combination of Venkatachary et al. (U.S. PG Pub No. 2004/0215956), in view of Sprague et al. (U.S. Patent No.5,247,575). Applicants respectfully transverse the rejection.

The Examiner alleges in the Office Action, that the Venkatachary et al. specification discloses "a method for providing access control management to electronic data, the method comprising establishing a secured link with a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is secured in a format including security information and an encrypted data portion, the security information including file key and access rules and controlling restrictive access to the encrypted data portion authenticating the user according to the identifier (see paragraphs 0011-0015, 0038, 0063-0069, 0076)."

The language of present claim 1 recites:

1. A method for providing access control management to electronic data, the method comprising:

establishing a secured link between a server providing the access control management and a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is not from the server but secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion;

authenticating the user according to the identifier; and

activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.

Claim 1 recites, in part, "***the authentication request*** including an identifier identifying a user of the client machine ***to access the electronic data.***" The Examiner contends that Venkatachary et al. teach "a method for providing access control management to ***electronic data.***" However, the portions of Venkatachary et al. cited by the Examiner do not disclose the current claim language. Venkatachary et al. disclose methods and systems for accessing networks (see the title of Venkatachary et al.) which allow a mobile user to access a network such as the Internet from a host network (see paragraphs 0011-0015).

Since the mobile user provides a username and password or other identifier to a database for authentication (see paragraphs 0011-0015, 0038, 0063-69), the mobile user is not sending "***the authentication request including an identifier identifying a user of the client machine to access the electronic data***" to the authentication mechanism (see paragraphs 0011-0015, 0038, 0063-69). In other words, the mobile user must first negotiate access and authentic to the host network, before the PANS server will recognize requests from the mobile user to access the Internet. Thus, the mobile user does not send an authentication request to access electronic data in the database.

Furthermore, when the mobile user attempts to access the Internet, authentication should have already occurred so any request sent to the Internet does not include an authentication request. Therefore, the mobile user is not accessing electronic data on the database, nor is the mobile users sending an authentication request to the PANS server when accessing the Internet. Thus, the Examiner has failed to demonstrate where Venkatachary et al. disclose this particular limitation of claim 1.

Applicants further contend that the relevant portions of Venkatachary et al. cited by the Examiner do not disclose accessing "electronic data, wherein the electronic data ***is not from the server***" providing the access control. Venkatachary et al. teaches that a mobile user typically establishes a communication link with the PANS server through an access point, and thereafter wirelessly transmits and receives data to and from the Internet

via the PANS server. The positioning of the PANS server in the subnet is such that data traffic from all users connected to this subnet goes through this server before reaching any other network, including the Internet (see paragraph 0012). Summarizing the previous argument, the mobile user does not send an authentication request to access electronic data in the database. Secondly, Applicants contend that Venkatachary et al. teach any request to and network packets from the Internet ***are from the server*** because the PANS server retrieves the network data from a requested server on the Internet.

Regarding the claim language accessing electronic data "***secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion,***" the Examiner points to encryption options for data packets that provide for no encryption to a very high level of encryption (see paragraph 0076). For example, the highest level of encryption might involve encrypting an entire data packet. A lesser level of encryption might involve encrypting only the header of each data packet or only a portion of the body of each data packet. Applicants contend that Venkatachary et al. do not disclose securing electronic data ***including security information and an encrypted data portion*** but encrypting network data packets. The network packets do not include ***a file key and access rules and controlling restrictive access to the encrypted data portion***. Thus, Applicants fail to see how a discussion of encrypting part or all of a network packet is equivalent to securing electronic data ***in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion.***

The Examiner further argues that Sprague et al. describes an information distribution system that remedies the deficiencies of the Venkatachary et al. reference. The Examiner contends that Venkatachary et al. does not disclosure "activating a user key ***after the user is authenticated***, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules." Concerning the Sprague et al. system, the Examiner concludes that it would have be obvious to one of ordinary skill in the art to modify Venkatachary et al. to include Sprague et al.'s inventive concept. Applicants respectfully disagree with this statement.

Venkatachary et al. disclose, in FIG. 4, a high level diagram of the authentication architecture for allowing access to the Internet. Particularly, in step 406, the mobile user is authenticated to the database. In step, 414 the PANS server generates a unique user token which is used in step 416 by the mobile users to communication with the PANS server. Venkatachary et al. state that authentication occurs before the PANS server will accept communication with the mobile user (see paragraphs 0011-0015), thus it is inherent that the unique user token is activated after the user is authenticated. The Applicants fail to see the Examiner's reasoning why one of ordinary skill in the art would be motivated to combine the Venkatachary et al. reference with the Sprague et al. reference because of an "inventive concept" in the second reference that is already present in the first reference.

Additionally, the Sprague et al. reference does not disclose that "the ***user key is used to access the access rules in the security information***, the file key can be retrieved ***to decrypt the encrypted data portion*** only if access privilege of the user is successfully measured by the access rules." The relevant portion cited by the Examiner discuss that at least a portion of the information stored in the first storage device is encrypted and the system comprises a device for decrypting the information selected and retrieved (column 6, lines 47-63, column 14 lines 11-29). The Applicants cannot identify how Sprague et al.'s method of encrypting information and providing a "device" for decrypting is equivalent to providing a user key "***to access the access rules in the security information***," whereby "***the file key can be retrieved to access the encrypted data portion***."

Specifically, Sprague et al. disclose in FIG. 3 a schematic representation of the format of the data stream. The data stream includes a security code 76 that permits access to the data to be restricted to a particular ***subset of user terminals*** by disabling decoding of the text by the security circuit. In other words, the security code provided by Sprague et al. provides access to the text of the data stream, and not "***to access the access rules in the security information***." Thus, the Examiner has failed to show that Sprague et al. teaches or discloses the limitations of claim 1.

Applicants submit that the Examiner has failed to establish a prima facie case of obviousness because the prior art references do not teach or suggest the claimed language

when the primary reference fails to disclose the present invention as claimed as is evident from the discussion above. Additionally, the Examiner has failed at meeting the two other prongs of the prima facie case of obviousness. Applicants submit that Examiner cannot show a suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Secondly, the Examiner has not provided a clear line of reasoning why the Applicants would modify a method of accounting and charging mobile users for access to the Internet over host networks to arrive at the present invention of securing a digital asset with security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion.

Based at least upon the above remarks, Applicants respectfully submit that claim 1 is allowable in view of Venkatachary et al. and Sprague et al., viewed alone or in combination, and request that claim 1 be allowed. Furthermore, since claims 2-15, and 17-19 depend from claim 1, Applicants submit that claim 2-15, and 17-19 are allowable in view of Venkatachary et al. and Sprague et al., viewed alone or in combination, for at least the same reasons given above in conjunction with claim 1, and request that claims 2-15, and 17-19 be allowed.

Independent claim 20 and dependant claims 21-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Venkatachary et al. in view of Sprague et al. The Applicants respectfully traverse this rejection.

Particularly the Examiner contends that Venkatachary et al. disclose the limitations of claim 20 using the same reference (see paragraphs 0011-0015, 0038, 0063-0069, 0076) as applied to claim 1.

Claim 20 recites, in part, that "maintaining a private key and a public key, both associated with the user, ***wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when or where the secured electronic data can be accessed*** and the encrypted data portion is an encrypted version of the electronic data." The Examiner

contends that Venkatachary et al. disclose securing electronic data with a header that includes ***controlling who, how, when or where the secured electronic data can be accessed***. The relevant portions cited by the Examiner clearly indicated that the encrypted network data passed between the mobile user and the PANS server only contains a unique key or token used to identify the mobile user and determine whether the mobile user has authenticated to user the Internet (see paragraphs 0011-0015, 0038, 0063-0069, 0076). In a more detailed reading, Venkatachary et al. disclose that the purpose of the key is to identify valid users and encrypt network packets from the user (see paragraphs 0070-0074, 0080-0081). Thus, the Examiner has failed to show how Venkatachary et al. disclose controlling "***how, when or where the secured electronic data can be accessed.***" The Examiner's reasoning why it would be obvious to one of ordinary skill in the art to modify Venkatachary et al.'s teaching to include Sprague et al.'s inventive concept is non-persuasive because Sprague et al. does not cure the deficiencies of Venkatachary et al.

Based at least upon the above remarks, Applicants respectfully submit that claim 20 is allowable in view of Venkatachary et al. and Sprague et al., viewed alone or in combination, and request that claim 20 be allowed. Furthermore, since claims 21-30 depend from claim 20, Applicants submit that claim 21-30 are allowable in view of Venkatachary et al. and Sprague et al., viewed alone or in combination, for at least the same reasons given above in conjunction with claim 20, and request that claims 21-30 be allowed.

Independent claim 31 and dependant claims 32-40 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Venkatachary et al. in view of Sprague et al. The Applicants respectfully traverse this rejection.

The Examiner similarly contends that Venkatachary et al. disclose the limitations of claim 31 using the same reference (see paragraphs 0011-0015, 0038, 0063-0069, 0076) as applied to claim 1 and claim 20.

Claim 31 recites, in part, "receiving a request to access the electronic data ***in a store***." Venkatachary et al. disclose, in the relevant portions cited by the Examiner,

accessing the Internet and do not disclose where the data from the Internet is stored. Moreover, as argued above with reference to claim 1, the mobile user must access the Internet and all network data through the PANS server that does not provide a store as claimed.

Claim 31 also recites, in part, "determining security nature of the electronic data by intercepting the electronic data moving ***from the store*** through an operating system layer to an application for the data." Venkatachary et al disclose, in the relevant portions cited by the Examiner, that the PANS server receives network packets from the mobile users over the network. Thus, Venkatachary et al. do not disclose receiving the electronic data from the store but from the network.

Again, as argued above with reference to claim 1, the Venkatachary et al. and Sprague et al. do not disclose "obtaining a file key and decrypting the encrypted data portion with the file key only after the user is determined to have the necessary access privilege to access the encrypted data portion, and thereafter the application receives the electronic data in clear form." The Applicants fail to see the Examiner's reasoning why there is a motivation to combine Venkatachary et al. and Sprague et al. from the fact that the Examiner did not include this and other claim language when making the rejection.

Based at least upon the above remarks, Applicants respectfully submit that claim 31 is allowable in view of Venkatachary et al. and Sprague et al., viewed alone or in combination, and request that claim 31 be allowed. Furthermore, since claims 32-40 depend from claim 31, Applicants submit that claim 32-40 are allowable in view of Venkatachary et al. and Sprague et al., viewed alone or in combination, for at least the same reasons given above in conjunction with claim 31, and request that claims 32-40 be allowed.

In paragraph 37 of the Office Action, the Examiner rejected claims 6-9, 26, and 27 under 35 U.S.C. §103(a) as being unpatentable over the combination of Venkatachary et al. (U.S. PG Pub No. 2004/0215956, in view of Sprague et al. (U.S. Patent No.5,247,575), in further view of Ozog et al. (U.S. PG Pub 2003/0033528). Applicants respectfully traverse the rejection.

Claims 6-9, 26, and 27 depend from claim 1 and claim 20. Based at least upon the above remarks, Applicants respectfully submit that claims 1 and 20 are allowable over Venkatachary et al. and Sprague et al. The addition of Ozog et al. does not cure the deficiencies of Venkatachary et al. and Sprague et al. In light of this, Applicants request that claims 6-9, 26, and 27 be allowed.

In paragraph 38 of the Office Action, the Examiner rejected claims 41-88 under the same rational as claims 1-40. Based at least upon the above remarks with respect to claims 1-40, Applicants respectfully submit that claims 41-88 are allowable in view of Venkatachary et al. and Sprague et al. and Ozog et al., viewed alone or in combination, and request that claims 41-88 be allowed.

CONCLUSION

Based on the foregoing remarks, Applicants believe that the rejections in the Office Action of November 3, 2004 and November 5, 2004 are fully overcome, and that the Application is in condition for allowance. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicants' undersigned representative at the number given below.

Respectfully submitted,
Alain Rossmann, et al.

Date: 2/3/05 By: Susan Yee

Susan Yee, Reg. No. 41,388
Carr & Ferrell LLP
2200 Geng Road
Palo Alto, CA 94303
Phone: (650) 812-3400
Fax: (650) 812-3444